SCIENCE

AND

TECHNOLOGY

FOR SECURING THE

HOMELAND

December 2004

Report of the Activities and Findings

by the Chairman and Ranking Member

Subcommittee on Cybersecurity, Science, and Research & Development

of the

U. S. House of Representatives Select Committee on Homeland Security

SCIENCE AND TECHNOLOGY FOR THE HOMELAND

INTRODUCTION

For over 50 years, the United States has remained a world leader, in part, because of its national commitment to and advancement of science and technology (S&T) to meet short-term and continuing national security needs. Today, the threats are closer to home. Terrorism, proliferation of weapons of mass destruction and disruption, and the spread of technology threaten our society and the way of life of each and every American citizen.

Terrorists will spend years planning their operations and believe they are in a long-term struggle that will take years, if not decades. The United States must be equally committed to pursuing a long-term strategy to develop technologies to prevent, mitigate, and respond to attacks in the future.

Whether it is investing in technology to detect and prevent clandestine nuclear materials from crossing our borders, or to assure that communications between our emergency responders are interoperable, research is necessary to overcome existing technical limitations and to provide protective systems that are important for a safer nation. To this end, Congress created a Directorate of Science and Technology within the Department of Homeland Security (DHS) in November 2002.

Developing and maintaining an enduring technological superiority is and will continue to be one of our first lines of defense. It is particularly important that the Science and Technology Directorate get it right, maintain a sense of urgency, and establish partnerships with the public and private sector to make sure we are tapping into the very best ideas, products, and research that this nation has to offer. We must continue to be aggressive, not just in pursuing this enemy, but in pursuing new technologies that will help keep our cities and towns more secure.

The U.S. House of Representatives created, in January 2003, a Select Committee on Homeland Security to improve coordination efforts and performance among Federal agencies tasked with protecting our homeland from terrorist attacks and to oversee the newly created Department of Homeland Security. The Subcommittee on Cybersecurity, Science, and Research & Development was created to oversee and help guide the Department's activities related to science and technology.

During the 108th Congress, the Subcommittee conducted several hearings and briefings for Members of Congress and staff on S&T issues. Oversight covered the gamut of S&T issues including encouraging the Department to develop tools to better assess and incorporate innovative ideas, products, and services from the private sector. Members of the Subcommittee wrote legislation to enhance the operations of the S&T Directorate. The other major product is this report—a bipartisan effort that highlights key science and technology issues and recommends a course of action for improving the Department of Homeland Security's effectiveness in these areas.

When DHS was created at the beginning of 2003, it inherited the mission and resources of numerous existing organizations. However, only a small number of personnel and functions previously existing within the Federal government were transferred into the Science and Technology Directorate. This provided the Directorate with a unique opportunity to create a new organization and hire employees to create an innovative organizational culture, a goal that the Directorate is on its way toward realizing.

As the Subcommittee completes its work in the 108th Congress, it presents findings and recommendations for future work on homeland security science and technology policy and legislation. These include requiring improvements in working with the private sector to vet good ideas and bring products to market, monitoring DHS's ability to work with other S&T elements across the Federal government that also research, develop, or deploy homeland security related technologies, and encouraging the Directorate to achieve the proper balance across its portfolios based on appropriate and valid threat and vulnerability assessments. Continued oversight from Congress and an organized effort from DHS are necessary to ensure homeland security priorities in science, technology, research, development, and procurement are met.

ROLE OF DHS

S&T Directorate Duties and Responsibilities

The S&T Directorate was created by Title III of the Homeland Security Act of 2002[i] and was first called for by the National Academies Report on Making the Nation Safer.[ii] The National Academies provided the President advice and counsel on "the complex interplay between technological, sociological and political issues." The National Academies maintained that the important role of science and technology in helping the nation meet its security needs was paramount. They believed that criteria for setting the nation's research priorities must be defined and they proposed new institutional arrangements and entities to enable stronger interactions between the nation's science enterprises. The Academies also stated that the nation's scientific enterprise is enormously complex with universities, government research laboratories and private industry all capable of providing quality R&D, but subject to an R&D vision that at the time was highly fragmented.

The key mission of the S&T Directorate[iii,iv] is to serve as the primary R&D arm of the Department of Homeland Security. This Directorate is directly responsible for ensuring homeland security research and development efforts associated with surveillance, prevention, detection, response, and recovery are appropriately prioritized, fulfill mission needs, are adequately funded, and meet near- and long- term Department-wide technology objectives. The S&T Directorate has the statutory requirement to leverage the historical strength of the vast scientific and technological resources of the nation, including the private sector and academic community, to help prevent and mitigate the effects of terrorism.

In addition, the S&T Directorate is to collaborate, coordinate, and partner with other Federal agencies, state, and local governments, and the private sector end-users, to identify requirements and develop and field capabilities to counter threats and improve counterterrorism operations. It must pursue innovative R&D and rapid prototyping/engineering for response systems. The Directorate must also maintain stewardship for homeland security research and development, investing in the necessary facilities, programs, and people to provide a stable base for the future.

The Department of Homeland Security Appropriations Act for Fiscal Year 2004 (P.L. 108-90) directed DHS to consolidate all Department-wide research and development (R&D) funding within the S&T Directorate. The Department has begun this consolidation and will continue these efforts in fiscal year 2005.

S&T Directorate Organization and Portfolios

Starting with a clean slate, the S&T Directorate organized its efforts into several categories and has used an organized budget and programming model similar to that employed by the Department of Defense. Four portfolios cover specific threats. Four portfolios address crosscutting issues related to those threats, and several portfolios support operational units within the Department. In addition, the Directorate also maintains other initiatives described below.

To carry out its work in the subject matter portfolios, The S&T Directorate established four key Offices:

- **Office of Plans, Programs and Budgets** – Develops strategic plans, budgets, and financial monitoring for specific portfolios, to include near-, mid-, and long-range research and development activities.

- **Office of Research and Development** – Uses other Federal government and academic resources to conduct long-term research, development, demonstration, testing, and evaluation of technologies to protect the homeland. This office provides stewardship to the scientific community and works to preserve and broaden the leadership of the United States in science and technology, coordinating with the National Laboratories, other Federal laboratories, research centers, and University Centers of Excellence.

- **Homeland Security Advanced Research Projects Agency** – Funds external research for the S&T Directorate. HSARPA uses multiple contracting vehicles and authorities to engage businesses, Federally-funded research and development centers, universities, and other government partners in an effort to gather and develop viable concepts for advanced technologies to protect the homeland.

- **Office of Systems Engineering and Development** – Implements and transitions large-scale or pilot systems to the field. This office's role is to identify and then reduce or eliminate risks associated with such technologies to ready them for deployment to the field.

In addition, the Homeland Security Act required the Directorate to establish a Federally Funded Research and Development Center (FFRDC) to assist the Department in formulating and addressing important homeland security issues, particularly those involving policy and security where scientific, technical and analytical expertise is required. The Department announced on April 23, 2004, that Analytic Services Inc. will operate this new Homeland Security Institute.

The Portfolios

Biological Countermeasures[v,vi,vii]

A terrorist attack involving biological weapons has the potential for catastrophic results, but is unique for the length of time involved between incident and effect. The nature of biological weapons therefore puts a premium on early detection and treatment, reflected in the S&T Directorate focus on enhancing biosurveillance. The BioWatch program provides a bio-aerosol warning system for dozens of metropolitan areas and DHS intends to expand and improve coverage and analysis; pilot an integrated attack warning and assessment system; and accelerate R&D for next generation sensors. The Information Analysis and Infrastructure Protection Directorate (IAIP) is working to integrate real-time biosensor data, information from health and agriculture surveillance programs, and terrorist threat and law enforcement information.

The S&T Directorate is working to develop and build the operational capabilities of the National Biodefense Countermeasures Center (NBACC) (Pronounced N-BACK). DHS is expanding as part of a planned biodefense campus at Ft. Detrick, MD, and will include new facilities for the National Institutes of Health's National Institute for Allergy and Infectious Diseases, as well as for the Department of Defense's U.S. Army Medical Research Institute of Infectious Diseases. NBACC, when operational, will support the law enforcement and intelligence communities in their biodefense responsibilities. The Center will apply the newest advances in science to the challenges both of biological threat characterization and of bioforensics, strengthening the nation's ability to determine the source of a biological agent used in an attack and strengthening deterrence

Radiological and Nuclear Countermeasures[viii]

The S&T Directorate's portfolio for radiological and nuclear countermeasures focuses on system analyses and pilot deployments for developing supporting information and analysis to deploy countermeasures; enhanced detection technology initiatives; product improvements to currently deployed detection systems; and enhancing capabilities in incident management and recovery.

The portfolio addresses the deliberate dispersal of small amounts of radioactive material from the detonation of an improvised or stolen nuclear weapon or as mixed with more conventional explosives. The development of technologies and systems to detect and interdict this material before it is used for malevolent purposes is of paramount importance. In addition, efforts in attribution, understanding where the material originated, is another key responsibility of the portfolio.

Chemical and High-Explosive Countermeasures[ix]

The chemical and high explosive countermeasure portfolio has the goal of developing capabilities to prevent and rapidly mitigate the consequences of chemical and high explosive attacks, improving explosive detection equipment, and enhancing response

plans. Other activities include developing and fielding equipment and technologies to interdict suicide bombers as well as car and truck bombs.

Threat and Vulnerability Testing and Assessment (TVTA)/ including Cybersecurity R&D[x]

The TVTA portfolio is developing and applying new technologies to improve terrorist threat assessment and understanding vulnerabilities. The portfolio is focused on providing the tools for evaluating extensive amounts of threat information, detecting and documenting this information, and coupling it with knowledge and assessments of critical infrastructure vulnerabilities.

Included in this portfolio is cybersecurity R&D, which supports the efforts of the Information Analysis and Infrastructure Protection Directorate. The National Cyber Security Division within IAIP is charged with improving security across the Federal government, to work with industry to secure major networks, and to, in particular, be able to support a 30-minute response time. The goal of those activities is to create, support, and strengthen a national and international cyberspace security readiness system, an information network to support crisis management during cyber and physical events, a national cyberspace security threat and vulnerability reduction program, and a national cyberspace security awareness and training program.[xi]

Standards/State and Local Programs and the SAFETY Act[xii]

Congress required the Department to develop and establish equipment standards as well as test and evaluation protocols for technologies. The S&T Directorate has also been charged with the implementation of the SAFETY (Support Anti-Terrorism by Fostering Effective Technologies) Act provisions, designed to encourage the development and rapid deployment of anti-terrorism technologies by limiting potential liability claims involving qualified technology. The S&T Directorate handles these responsibilities within the Standards and State and Local Programs portfolio.

The Directorate continues to work with nongovernmental standard-setting groups, interagency teams, and the Office of Science and Technology Policy to develop national standards for biological detectors. Standards for four classes of radiation detectors are planned for fiscal year 2005.

Emerging Threats[xiii]

The goal of the Emerging Threats portfolio is to develop capabilities to identify, assess, and provide security for new and emerging terrorist threats and to employ technological developments for the advancement of homeland security.

Rapid Prototyping[xiv]

The Rapid Prototyping portfolio is tasked with developing, prototyping and commercializing innovative technologies. This includes identifying, assessing, and selecting candidate technologies. Currently, the Directorate is using the Technical Support Working Group (TSWG) to provide such technical assistance, but may plan to reduce the role of TSWG in fiscal year 2005 and provide much of those services in house.

Support of DHS Conventional Missions[xv]

The S&T Directorate, in addition to conducting and supporting research and development activities, is also given the responsibility to meet the technological needs of other DHS components. Activities include enhancing technologies for surveillance and monitoring land and sea for potential terrorist activity, emergency preparedness, and screening and detection for traditional missions at the border and ports of entry.

Other Activities

Counter-MANPADS[xvi]

The Directorate, through its Office of Systems Engineering and Development, is identifying, developing and testing a cost-effective capability to protect the nation's commercial aircraft against the threat of man-portable air defense systems. Development contracts were started in fiscal year 2004 to prepare the conceptual framework for the overarching programs and will continue in fiscal year 2005. Mature technologies to protect commercial airliners were to be evaluated in fiscal year 2004, including preliminary design reviews of systems concept, requirements analysis and preliminary design information. Phase II will require contractors to finalize design, test the design, provide aircraft integration of defense systems on commercial aircraft, and support a test and evaluation activity of the defense capability.

University Programs/ Fellowship Programs[xvii]

Collaboration with academia is vital to a robust research and development program. The Homeland Security Act called for DHS, "...to establish a coordinated, university-based system to enhance the nation's homeland security," to attract and retain the nation's best and brightest academics, and to help provide an enduring capability for the new counterterrorism mission. The University Programs component of the Office of Research and Development involves two programs: the development of ten University Centers of

Excellence intended to study homeland security-related issues for three years each, and the Homeland Security Scholars and Fellows program to attract university students and graduates to careers in homeland security.

Interoperability[xviii]

Project SAFECOM (Wireless Public SAFEty Interoperable COMmunications Program) is an e-government initiative and is funded on a multi-agency cost-share plan. DHS is the managing partner for SAFECOM, with contributing partners including the Departments of Justice, Treasury, Agriculture, Defense, Transportation, Energy, Health and Human Services, and Interior.

The S&T Directorate's Project SAFECOM role is to provide Federal, state, and local public safety agencies with central coordination, leadership, and guidance to help them achieve short-term interoperability and long-term compatibility of their radio networks across jurisdictions and disciplines.

In addition, DHS has created the Office of Weapons of Mass Destruction Operations and Incident Management to offer scientific advice and support for crisis operations. This office provides support to the DHS Secretary in assessing and responding to threats against the homeland.

Science & Technology Directorate Activities

Since its inception in March 2003, the S&T Directorate has worked to develop coordinated research initiatives across the public and private sector scientific communities to make progress on the highest priority issues, including biological, chemical, and radiological/nuclear countermeasures; risk assessment and risk communication; and rapid response. While more work remains to be done across multiple homeland security disciplines, some of the Directorate's accomplishments are described below.

Protecting the Nation from Biological and Chemical Threats:

- On January 29, 2004, the Homeland Security and Health and Human Services Secretaries announced a $274 million Bio-Surveillance Program that improves ongoing programs in human health, hospital preparedness, state and local preparedness, vaccine research and procurement, animal health, food and agriculture safety, and environmental monitoring.

- The S&T Directorate and the Washington Metropolitan Area Transit Authority (WMATA) recently completed PROTECT (Program for Response Options and Technology Enhancements for Chemical/Biological Terrorism). PROTECT, which is an operational chemical agent detection and response capability program, is deployed in certain metro stations and operated by WMATA. Upon completion, the system will be totally owned and operated by WMATA and expanded to approximately 20

stations. The information gleaned from PROTECT will have direct applications to similar facility protection and response efforts across the nation.

Using Science and Technology to Assist First Responders:

- In April 2004, DHS released the first comprehensive Statement of Requirements that provides the public safety community with a shared vision and describes how first responders can use in-the-field information resources more efficiently when responding to a variety of emergencies. This is the first time the 50,000 public safety agencies have a document that defines future requirements for communicating and sharing information, and complements the grant guidance DHS already put in place for communications equipment.

- Setting Standards: Working with the emergency responder community and national voluntary standards organizations, on February 26, 2004, the S&T Directorate unveiled its first set of standards related to personal protective equipment for fire fighters. Initial guidelines for radiation detection technology have already been made available, with formal standards nearing completion. Other standards are expected to be released in 2005.

Finding Innovative Ways to Secure Our Borders and Ports and Transportation:

- The S&T Directorate began a research project to develop techniques to determine whether an individual has been handling radioactive materials or has been immunized against or exposed to dangerous pathogens or chemicals. If this project is successful, techniques could be integrated into procedures already in place at U.S. borders and would allow officials to determine if there are any indicators of potential terrorist activity.

- The S&T Directorate now manages the Port Authority of New York and New Jersey's radiation detection test bed to test and evaluate individual pieces of detection technology and develop response protocols and operational concepts. Radiation detection equipment has been installed at tunnels, bridges, ports, and airports in the New York City metropolitan area. Scientists, engineers and operators working together will lead to better decisions on detection technology R&D investment, deployment of urban monitoring systems, configurations best able to enhance security, and viable solutions for protecting the nation from radiological and nuclear threats.

- The S&T Directorate initiated the Border Safe Integrated Feasibility Experiment. This experiment creates an infrastructure in the Southwest U.S. for data sharing between the Department's Border and Transportation Security Division and local and state law enforcement officials. The resulting system will identify individuals who have already entered our country, either legally or not, and who engage in hostile

behavior after crossing the border. Tucson AZ and San Diego CA are already sharing information and working with Customs and Border Patrol offices there. The effort is a joint technology development program among these participants.

- The S&T Directorate has joined with the U.S. Coast Guard to build a prototype integrated maritime surveillance system covering Port Everglades, Miami, and Key West, Florida. The $4.0 million, 24-month program will integrate existing facilities and upgrade equipment to detect, track, and identify vessel traffic around ports, in the zones around ports, and over the horizon. This evolutionary testbed will provide an immediate coastal surveillance capability in a high priority area and offer the U.S. Coast Guard and other Departmental organizations the means to develop operational concepts, and implement and test interoperability among Homeland Security and Department of Defense systems and networks.

- The S&T Directorate provides a "reachback" capability for the Department's radiation detectors across the country. Through this service, scientific experts in the S&T Directorate can assist security personnel in the field to resolve questions when detectors identify a radiation source and when there is a case of potential nuclear smuggling. The interaction with personnel working with deployed detectors also helps the Directorate improve the quality of radiation detection devices. Initially implemented in August 2003 with the Department's Customs and Border Patrol as the primary customer, this program now provides assistance to the entire Department, and outside agencies.

Using Technology to Share Information and Safeguard Critical Infrastructure:

- The S&T Directorate established a Federal Government-wide Steering Group, comprising 22 agencies from the Intelligence and Law Enforcement Communities, to collaborate on research activities relating to information analysis and sharing. One of the immediate results of that coordination was the establishment of an Inter-agency Center for Applied Homeland Security Technology (or ICAHST). The ICAHST will be used as a test bed to investigate and evaluate new technologies and techniques and validate user requirements.

- The S&T Directorate has established a Biodefense Knowledge Center (BKC) to serve as a clearinghouse for sharing and analyzing information on biological threats – with the NBACC, the intelligence community agencies, law enforcement agencies on the Federal, state, and local level, and public safety and public health agencies.

Partnering with Industry:

- The Homeland Security Advanced Research Projects Agency has completed two major solicitations for technology proposals. The first announcement resulted in 3344 proposals that led to 55 signed contracts to date. The second solicitation was issued for chemical and biological sensors to upgrade BioWatch sensors and systems, enable smart buildings, and support emergency responders. Seventeen awards have been made to date for promising prototypes. Radiological and Nuclear Detection and Architecture solicitations have been published.

- DHS is also reaching out to small business innovators. Over 60 firms received a total of $6.5 million, with individual firms each receiving up to $100,000 for a period of six-months to develop new technologies.

- To date, the Office of SAFETY Act Implementation[xix] has received 35 full applications and 126 pre-applications. The Department awarded SAFETY Act designation and certification to four companies: Lockheed Martin, Michael Stapleton Associates, Northrop Grumman and Teledyne Brown.

Creating a Science and Technology Infrastructure:

- To provide stewardship to national homeland security capabilities, the S&T Directorate:
    - Developed the framework for the Homeland Security National Laboratory System comprised of DOE National Laboratories.
    - Named, in September 2003, 100 students to the inaugural class of the Department of Homeland Security's Scholars and Fellows Program. This program supports students who are attending universities across the country majoring in the physical, biological, social and behavioral sciences, including science policy, engineering, mathematics, or computer science.
    - Established three University Centers of Excellence to foster homeland security mission-critical research and education. Texas A&M University and the University of Minnesota are leading two Homeland Security Centers of Excellence (HS-Centers) on agricultural security. The University of Southern California was chosen to conduct risk analysis related to the economic consequences of terrorist threats and events. A fourth university center on behavioral aspects of terrorism will be announced shortly.

Working with International Partners:

- S&T leadership established working relationships with officials of several foreign governments, including Great Britain, Israel, Japan, Canada, and Mexico. Workshops are also scheduled with several delegations to explore areas of cooperation.

- In October 2003, Secretary Tom Ridge and Canadian Deputy Prime Minister John Manley initialed an agreement on Science and Technology Cooperation for protecting

shared critical infrastructures and enhancing border security. U.S. and Canadian officials are working to develop technologies to: protect bridges, dams, pipelines, and communications and power grids; enhance the ability to disrupt and interdict terrorists through surveillance and monitoring; and detect the illicit transportation of chemical, biological, radiological, and nuclear weapons.

SUBCOMMITTEE OVERSIGHT

Subcommittee Jurisdiction

Responsibilities for the Subcommittee on Cybersecurity, Science, and Research & Development include authorization and oversight of the Department's activities related to security of computer, telecommunications, information technology, industrial control, electric infrastructure, and data systems, including science and research and development; protection of government and private networks and computer systems from domestic and foreign attack; and prevention of injury to civilian populations and physical infrastructure caused by cyber attack. The Subcommittee also was established to, among other things, provide oversight of the science and research and development of prevention, protection, detection, response, and recovery countermeasures to biological, chemical, radiological, nuclear and high explosive threats.

Subcommittee Membership

Mac Thornberry, Texas, Chairman
Pete Sessions, Texas, Vice Chairman
Sherwood Boehlert, New York
Lamar Smith, Texas
Curt Weldon, Pennsylvania
Dave Camp, Michigan
Robert W. Goodlatte, Virginia
Peter King, New York
John Linder, Georgia
Mark Souder, Indiana
Jim Gibbons, Nevada
Kay Granger, Texas
Christopher Cox, California, ex officio

Zoe Lofgren, California, Ranking Member
Loretta Sanchez, California
Robert E. Andrews, New Jersey
Sheila Jackson-Lee, Texas
Donna M. Christensen, U.S. Virgin Islands
Bob Etheridge, North Carolina
Ken Lucas, Kentucky
James R. Langevin, Rhode Island
Kendrick B. Meek, Florida
Ben Chandler, Kentucky

Jim Turner, Texas, ex officio

Subcommittee Activities

Oversight

Over the past year and a half, the Subcommittee has focused on examining both the overall mission of the Science and Technology Directorate of the Department of Homeland Security and specific research and development activities of concern. Three hearings since April 2003 focused on the S&T Directorate mission and research portfolios. In addition, a full Committee hearing on Biodefense was held in May 2004

and two Subcommittee member briefings were conducted on radiological and nuclear detection and interoperable communications.

The Subcommittee provided oversight of the offices within the S&T Directorate with special emphasis on the research and development direction of the biological threat countermeasure portfolio and the establishment of the National Biodefense Analysis and Countermeasure Center (NBACC). In addition, the Subcommittee obtained information on the technology development and transfer efforts of the Homeland Security Advanced Research Projects Agency; major systems engineering projects such as BioWatch and the New York, New Jersey Port Authority detector test bed project; the relationship between DHS and the Technical Support Working Group (TSWG); the research portfolio of the Plum Island Animal Disease Center; the activities of the university center program; the radiological and nuclear countermeasure portfolio, and the progress in the counter man-portable air defense systems (Counter-MANPADS) project.

Other visits and briefings focused on geospatial initiatives of the Federal government and the role of DHS in geospatial management in support of homeland security. Finally, several staff briefings were held to solicit industry and Federal input on establishing performance measures for highly integrated organizations.

As a result of its work during the 108th Congress, the Subcommittee finds that the S&T Directorate:

- has made significant progress in establishing its organizational and management structure and obtaining personnel;
- is beginning to use the resources of the national and Federal laboratories to meet the technical needs of the Department;
- is developing a mechanism to work with academic institutions to ensure a pipeline of scientists, engineers, and other students interested and committed to studying and applying their knowledge to the nation's homeland security;
- is utilizing the private sector in order to develop and move countermeasure technology in specific areas to the end-user, but needs to expand this effort and improve outreach;
- is not fully utilizing its statutory authority for engaging the private sector on technological solutions and expertise in the transfer and commercialization of promising technologies for use by all levels of government and the private sector; and
- should address organizational and process issues to improve its performance in technology transfer, long term research supporting emerging threats, and interoperable communications.

Hearings

Preparing for the Future

On May 21, 2003, the Subcommittee on Cybersecurity, Science, and Research & Development held an oversight hearing entitled "Homeland Security Science and

Technology: Preparing for the Future." Testimony was received from: the Honorable Charles McQueary, Ph.D., Under Secretary for Science and Technology, Department of Homeland Security. This hearing provided valuable insight into how the Department was getting organized, establishing priorities, and dealing with the extensive breadth of research and development required to cover a myriad of issues for the homeland.

Radiological and Nuclear Detection

On Thursday, September 25, 2003, the Subcommittee on Cybersecurity, Science, and Research & Development received a joint briefing with the Subcommittee on Emergency Preparedness and Response and the Subcommittee on Infrastructure and Border Security on "Radiological and Nuclear Detection: Is Science Saving the Day?" Representatives from the Department of Homeland Security, the national laboratories and the Port Authority of New York and New Jersey briefed Members and staff on technological advancements and application in detection of radiological and nuclear components. The briefing was presented by Dr. Maureen McCarthy, Director, Office of Research and Development; Mr. Ray Vitkus, Group Leader of Nonproliferation and International Technology Group, Los Alamos National Laboratory; Dr. Page Stoutland, Program Leader, Radiological and Nuclear Countermeasures, Lawrence Livermore National Laboratory; and Mr. Brian Lacey, Office of Operations and Emergency Management, the Port Authority of New York and New Jersey.

Communications Technology Interoperability

On Wednesday, October 15, 2003, the Subcommittee on Cybersecurity, Science, and Research & Development and the Subcommittee on Emergency Preparedness and Response received a joint briefing on "Communications Technology and Interoperability: Can Science and Technology Help Overcome Communications Obstacles for First Responders?" This briefing was important to update the Subcommittee on technological issues associated with First Responder communications, such as radio frequency spectrum, common infrastructure standards to allow for communications across regional and state boundaries, and the need for exercises to practice emergency coordination during times of crisis. The briefing was presented by Dr. David Boyd, Director, SAFECOM Program Office; Gary Grube, Chief Technology Officer, Motorola; and the Hon. Edward Flynn, Secretary of Public Safety, Commonwealth of Massachusetts.

Science and Technology in DHS

On Thursday, October 30, 2003, the Subcommittee on Cybersecurity, Science, and Research & Development held a hearing entitled "Strength Through Knowledge: Homeland Security Science and Technology Setting and Steering a Strong Course." Testimony was received from the Honorable Penrose C. Albright, Assistant Secretary for Plans, Programs and Budgets, Department of Homeland Security.

Science and Technology Budget FY 2005

On Wednesday, February 25, 2004, the Subcommittee on Cybersecurity, Science, and Research & Development held a hearing entitled "The Homeland Security Science and Technology Budget Hearing for Fiscal Year 2005." Testimony was received from the Honorable Charles McQueary, Under Secretary Science and Technology, Department of

Homeland Security. A comprehensive budget plan was presented for the coming year, demonstrating strategic plans to address vital homeland research issues and priorities.

Legislative Activities

Chairman Thornberry and Ranking Member Lofgren introduced H.R. 5069, The Department of Homeland Security Science and Technology Enhancement Act of 2004, on September 13, 2004. The purpose of the legislation is to improve DHS organizations and processes. The legislation focused on cross-cutting issues of integration and coordination, organizational and process improvement, effective technology transfer, and long-term investment in research and development. Several provisions of the bill include:

- authorizing the Secretary of Homeland Security to establish and maintain special access programs associated with research, development, test and evaluation, and acquisition of technology;
- directing: (1) the Secretary to submit to Congress certain budget request information for the Directorate of Science and Technology; and (2) the Under Secretary for Science and Technology to transmit to Congress a summary of the solicitations and resulting contracts and grants awarded in the past fiscal year.
- requiring the Secretary to conduct an assessment of: (1) the development of national capabilities in homeland security science and technology; and (2) the methods used by the Directorate for the prioritization of science and technology projects among and within research portfolios;
- directing the Secretary to establish a program to award grants to institutions of higher education for: (1) the establishment or expansion of professional development programs and associate degree programs in cybersecurity; and (2) the purchase of equipment to provide training in cybersecurity for either professional development or degree programs;
- authorizing the Secretary to enter into agreements or partnerships with foreign governments that are U.S. allies in the war on terrorism and have extensive experience in counterterrorism;
- directing the Secretary to establish: (1) a Geospatial Management Office; and (2) a program to enhance public safety interoperable communications. (These two provisions were subsequently incorporated into the Intelligence Reform and Terrorism Prevention Act of 2004 (December 17, 2004; 118 Stat.3638; P.L. 108-458); and
- providing for the establishment of a homeland security technology and equipment transfer program.

Legislative Chronology

H.R. 4852 was introduced July 19, 2004, as the "Department of Homeland Security Authorization Act for Fiscal Year 2005."

- Title III – Science and Technology

H.R. 5069 was introduced September 13, 2004, as the "Department of Homeland Security Science and Technology Enhancement Act of 2004."

S.2845 was signed into law, December 17, 2004 as the "Intelligence Reform and Terrorism Prevention Act of 2004."

- Enhancing interoperable communications for the nation's first responders
- Geospatial organization and coordination

ROADMAP FOR THE FUTURE

During the 108th Congress, the Subcommittee was guided by two primary principles. First, the nation's S&T efforts to combat terrorism must be strengthened. Secondly, DHS should be encouraged to use, to the fullest extent possible, private industry and the academic community to develop and transition technologies to Federal, state, regional, local and private sector entities. These two objectives remain salient for the coming year.

Specifically, in the area of strengthening the nation's science and technology, the Subcommittee should continue to work to ensure that DHS:

- invests in research, development, test and evaluation for science and technologies in prevention, detection, response, and recovery;
- balances the science and technology countermeasure portfolios based on appropriate and valid threat and vulnerability assessments;
- uses the resources of our national and Federal laboratories;
- enables capability through university centers and fellowship programs; and
- develops a national infrastructure through Federal stewardship to support a long-term capability to counter threats.

To encourage DHS to use private industry to develop and transition technologies to the Federal, regional, state, local, and private sector end user, the Subcommittee should encourage and work with the Department to:

- establish a Technology Clearinghouse and technology transfer program to quickly solicit, develop, evaluate and transfer technologies;
- move technologies quickly to market by engaging in rapid prototyping and implementing the SAFETY Act to limit liability risk for qualified technologies; and
- develop standards for countermeasure technologies so industry can move forward in developing and commercializing technologies that are, if required, interoperable.

In addition to these overarching principles, the Subcommittee should continue oversight and coordination with the Department to determine:

- how well the Department is identifying and fielding existing technologies that are needed for homeland security;
- how the Department is conducting research and development in areas that are needed but do not presently exist;
- how the Department is setting priorities for resource allocation;
- how new ideas are received from the private sector and incorporated into overall R&D planning, and if DHS is providing feedback to industry; and
- how DHS is organized and staffed to meet these challenges.

Below are some additional areas for the Subcommittee and Congress to consider in the 109th Congress to enhance the S&T Directorate's functioning.

Integration and Coordination

One of the prime lessons learned from private sector mergers is the importance of creating a "company culture" in the first few months of the transition. Although this merger process has been slow across the Department of Homeland Security, the S&T Directorate was not burdened by legacy agency integration issues, so it was able to move forward more quickly.

The S&T Directorate's success is dependent on how well it supports the missions of the operational agencies within DHS, ensuring that the best science is done, the most promising technologies are being developed, and the most capable systems are procured and deployed. The Directorate also has an interest in leveraging research and development for one aspect of homeland security to other areas. This can be done most effectively and with the minimum of unnecessary duplication if the R&D work of the Department is consolidated in the S&T directorate. The Department has made progress in this consolidation effort by bringing in elements associated with the Coast Guard R&D and other emergency response-oriented work. Significant R&D efforts, however, remain outside the Directorate, including R&D for the Department-Wide Technology Investment program, the Secret Service, Border and Transportation Security (e.g., US VISIT Program), Customs and Border Protection (e.g., Automation Modernization Program), the Information Analysis and Protection Division, and the Transportation Security Administration. The Subcommittee encourages the Department to complete this consolidation wherever beneficial.

Technology: Transferring Technology to Operational End-Users Quickly and Efficiently

The ability to do the best science, develop the most promising technology, and demonstrate and deploy the best countermeasures in a timely and efficient way is essential. Tools must be available to tap the extraordinary capability and ideas that exist in Federal departments, at all levels of government, universities, and private industry. Processes must be developed to assure rapid research development and test and evaluation, delivery or transfer of the technology, and commercialization. Finally, sound management and governance practices at all levels of government are needed to appropriately deploy technology at our borders, ports and critical infrastructures.

DHS must also continue to develop sound standards for technologies and implement a streamlined certification process in implementing the SAFETY Act. It was Congress' intent that the SAFETY Act assist in getting critical antiterrorism technologies to the market place; however, there continues to be concern with the Directorate's implementation of the SAFETY Act. It is important that implementation not be unnecessarily complicated, speculative, or burdensome.

Joint Development of Counterterrorism and Homeland Security Technologies, Products, and Services

The Subcommittee recognizes that nations other than the United States have had significantly longer experience with terrorist attacks on their homeland and have developed expertise in science and technology for security purposes. In recognition of this fact, the Directorate should increase its efforts to engage in collaborative efforts with foreign governments, especially those of Israel and the United Kingdom, to jointly develop counter-terrorism and homeland security technologies, products, or services.

Measuring Performance

The Department, with help from Congress, must be accountable to the American people by answering the fundamental question of how it is helping to make the country safer. It is important for the S&T Directorate to develop metrics to evaluate its progress and continuing needs. Some of these measures will be fairly easy: the number of standards promulgated or technologies transferred can be easily counted and impacts judged. Others, such as measuring progress in the development of a stable national technology base for homeland security, may be more difficult. Given the importance of this task, however, the Directorate must develop meaningful measurements of its performance.

Special Access Program

The Subcommittee recommends that the Secretary be authorized to establish and maintain special access programs associated with the research, development, testing, evaluation, and acquisition of technology or systems, subject to the reporting requirements that exist for such programs elsewhere in the federal government.

The Subcommittee recognizes that certain research, development, testing, evaluation, and acquisition of technology or systems, if broadly disclosed , could possibly cause severe damage to the national or homeland security of the United States. To that end, the Subcommittee recommends that the S&T Directorate be authorized to use special access programs. Because of the potential for misuse of special access programs, Congress should conduct vigorous oversight over the S&T Directorate's use of them if authorized. The Subcommittee continues to believe that, to the greatest extent practicable, research conducted or supported by DHS should remain unclassified.

Additional Budget-Related Submissions

The Subcommittee recommends that, beginning in fiscal year 2006 and annually thereafter, the Secretary submit specialized budget information for the S&T Directorate simultaneously with the submission of the President's annual budget request. Such Directorate-specific budget request information should include not only research portfolio-based budget submissions, but also estimated funding summaries for each of the

following: the Office of Research and Development, the Office of Homeland Security Advanced Research Projects Agency, the Office of Systems Engineering and Development, the Office of Plans, Programs, and Budget, and such other major Directorate components as the Secretary may establish.

At present, DHS submits the S&T Directorate's research and development budget request primarily by programs organized by specific research portfolios. The Subcommittee would benefit from Directorate budget submission information on its various "administrative elements" as well as its "research portfolios" in order to achieve a more complete understanding of how the Directorate spends its research funding.

A budget request by research portfolios and estimated funding summaries by administrative elements will allow Congress to understand fully each research area and to track the status and the amount of money being spent on programs at various stages of the research and development process -- from scientific discovery to operational testing. This change in DHS' budget submission also will permit some transparency into the relative efforts of the private sector, educational institutions, and the Federal government. In addition, the Subcommittee recommends that the Directorate include budget requests that reflect commitments from other Department Directorates for the purchase and/or the deployment of technologies developed by or in development in the Department.

Balanced S&T Portfolio

No threat countermeasure system is foolproof. Countering terrorism requires a layered defense that balances work in surveillance (intelligence), prevention, detection, response (including attribution) and recovery. It is understandable that high consequence threats, such as nuclear or biological events, receive significant attention given their potential for damage. However, DHS must determine the probability of all threats and be confident in its consequence assessments. While difficult, it is important to develop a scientific basis for this determination in order to prioritize research and technology development and to influence our nation's preparedness for these threats. Lower consequence threats cannot be ignored. Although potentially not catastrophic, these threats can undermine the security and psyche of the nation. These consequences must be adequately evaluated such that appropriate investments in countermeasures are made.

The Subcommittee recognizes that much of the S&T Directorate's work is complemented by efforts underway in other Federal departments, especially in the areas of biological, radiological and nuclear terrorism. We therefore recommend that the Secretary, in consultation with the Secretaries of appropriate Federal agencies, develop a comprehensive national strategy to address the biological threat and the radiological/nuclear threat.

Each strategy should set forth the objectives, missions, and priorities for defense in the context of prioritized biological and radiological/nuclear threats to and vulnerabilities of the nation. The strategy should specify the objectives, missions, and priorities of each Federal agency with research and development responsibilities as well as other

responsibilities such as surveillance, threat and risk analysis and incident response. A description of these responsibilities and the mechanism by which the Federal agencies coordinate their efforts should be provided as well.

The Subcommittee believes that the strategies should describe the role of state and local governments and private sector institutions. An important component of the strategy should also be the performance benchmarks developed to measure progress in achieving the objectives of the strategy with expected timeframes for implementation.

Interoperable Communications and Geospatial Information

The Subcommittee recommends continued oversight of the provisions regarding interoperable communications and geospatial information in the Intelligence Reform and Terrorism Prevention Act of 2004 to ensure compliance with the legislation and to consider additional actions if necessary. Further, the Subcommittee believes all funding for Project SAFECOM should be appropriated directly to DHS in order to avoid the delay that Project SAFECOM has historically experienced in receiving funds from other Departments or agencies.

Long-Term Research to Develop, Maintain and Sustain a Robust Capability

DHS is currently focused on short-term investments and near term successes in developing and deploying countermeasures; however, the nation must stay ahead of terrorist threats rather than be reactive. The development of next generation countermeasure technologies requires long-term research investments in the enabling science – some of it in basic research – that will allow DHS to anticipate or better respond to emerging threats. DHS has identified that basic research constitutes eight percent of the activities within the S&T Directorate. DHS should devote more resources to this basic research work, both through work conducted by DHS personnel and through increased support to academia and elsewhere.

Research and Development Prioritization

The Subcommittee recommends that the Secretary assess the development of national capabilities in homeland security-related science and technology. As part of that assessment, the Secretary should identify the most important scientific and technological challenges and priorities and the extent to which DHS' research and development agenda is addressing them. Moreover, the Secretary should assess the effectiveness of DHS' coordination of other Federal homeland security-related R&D associated with such challenges and priorities, and whether the basic research agenda and science investment will meet the nation's long-term homeland security needs.

Similarly, the Secretary should assess the methods used by the S&T Directorate for the prioritization of science and technology projects among and within research portfolios, including the selection and execution of such projects. As part of such an assessment, the Secretary should evaluate the following: (1) the process for obtaining classified and unclassified threat and vulnerability information and how that information is used to inform decisions on resource and funding allocations; (2) the usefulness of following a cost/benefit analysis to allocate funding among research portfolios and other Directorate components; and (3) the methods used for selecting, funding, and awarding homeland security science programs at the national laboratories and academic institutions and whether optimal use of these entities is being made.

Technology Development and Transfer

The Subcommittee recommends that the S&T Directorate greatly enhance its technology clearinghouse required under section 313 of the Homeland Security Act by establishing a homeland security technology and equipment transfer program to facilitate the identification, modification, and commercialization of existing technology and equipment for use by Federal, state and local governmental agencies, emergency response providers, and the private sector.

The Directorate should conduct surveys and review technologies that DHS, other Federal agencies, or the private sector have developed, tested, evaluated, and demonstrated and that may prove useful in assisting homeland security and emergency response officials at all levels of government and the private sector. The Directorate should conduct or support tests, evaluations, and demonstrations, as appropriate, of technologies identified through such surveys, including any necessary modifications to such technologies for counter-terrorism use. As progress is made in technology transfer, the Directorate should assess the value of taking on the role of validating technologies or contracting that effort to ensure technologies meet the needs of the end users and incorporate some degree of interoperability.

The Subcommittee underscores the importance of the Directorate's full utilization of its statutory authority related to the Technology Clearinghouse to engage the technological solutions and expertise of the private sector. The transfer and commercialization of promising technologies for use by Federal, state, and local governmental agencies, emergency response providers, and the private sector will continue to enhance the nation's capabilities to prevent, prepare for, respond to, and recover from terrorist attacks. To further facilitate this development, the Subcommittee specifically encourages continued interaction with the Department of Defense (DoD) to identify and adapt military technologies that have homeland security applications and to incorporate promising technology into the technology transfer program.

In addition, engaging the private sector by thoroughly assessing unsolicited proposals, and by being accessible and responsive to private sector entities with potentially innovative homeland security technologies, minimizes duplications, expedites transfer of technology to emergency responder providers, and maximizes the use of existing

technology solutions for homeland defense. The Subcommittee is concerned with how the Department is handling unsolicited proposals. There continues to be complaints regarding unresponsiveness on the part of the Department to enterprising companies. These concerns should be addressed.

CONCLUSION

The Science and Technology Directorate of the Department of Homeland Security has a critical role of developing new technologies and procedures to enhance our nation's homeland security. This entails both developing new products and services for use at the federal, state, and local level as well as serving as the scientific advisors for the rest of the Department.

Unlike most of the Department, the Directorate was created mostly as a new entity and not as a collection of previously disparate agencies. This beginning has allowed the Directorate to forge a common culture and operate as a cohesive whole, but also accounts for a delay as it develops internal mechanisms and the tools to accomplish its mission. The Subcommittee looks forward to assisting the Directorate in completing its initial development period by providing the authorities and resources needed and through strong oversight of Directorate activities.

In its first two years, the S&T Directorate has several accomplishments, some of them outlined in this report, that have and will continue to enhance the nation's homeland security. There are also several areas that still need improvement, including better processes and attention to working with the private sector and mechanisms to transfer technologies to them. Additionally, developing and maintaining an enduring technological superiority is and will continue to be one of our first lines of defense in homeland security.

Today the Department of Homeland Security is working to make the nation safer than it was in the days preceding and immediately following the terrorist attacks on our homeland in September 2001. The men and women of the Department are joined in this effort with personnel in other government agencies, state and local first responders, businesses, and individual citizens. Our ability to protect borders, bolster transportation security, improve first responder capabilities, and improve other security activities will depend on the nation's ability and devotion to maintaining our lead in science and technology.

ENDNOTES

[i] Homeland Security Act of 2002, Public Law 107-296, November 25, 2002

[ii] Making the National Safer, the Role of Science and Technology in Countering Terrorism, by the National Research Council of the National Academies, 2002

[iii] Subcommittee on Cybersecurity, Science, and Research and Development Hearing, "Homeland Security Science and Technology: Preparing for the Future, May 21, 2003, Witness: the Honorable Charles McQueary, Ph.D.

[iv] Subcommittee on Cybersecurity, Science, and Research & Development Hearing, "Strength through Knowledge: Homeland Security Science and Technology- setting and Steering a Strong Course, October 30, 2003, Witness: Dr. Penrose (Parney) C. Albright.

[v] Department of Homeland Security Science and Technology Fiscal Year 2005 Congressional Budget Justification

[vi] Department of Homeland Security Information Analysis and Infrastructure Protection Fiscal Year 2005 Congressional Budget Justification

[vii] Executive Office of the President Office of Management and Budget (OMB), Budget for Fiscal Year 2005

[viii] Department of Homeland Security Science and Technology Fiscal Year 2005 Congressional Budget Justification

[ix] ibid

[x] ibid

[xi] Department of Homeland Security Information Analysis and Infrastructure Protection Fiscal Year 2005 Congressional Budget Justification

[xii] ibid

[xiii] Department of Homeland Security Science and Technology Fiscal Year 2005 Congressional Budget Justification

[xiv] ibid

[xv] ibid

[xvi] Department of Homeland Security Science and Technology Fiscal Year 2005 Congressional Budget Justification

[xvii] ibid

[xviii] ibid

[xix] email from Rachel Williams, S&T Directorate Legislative Affairs, summarizing Safety Act information from Ms. Wendy Howe, Director of the Office of Safety Act Implementation, 9/21/04